NORTH-HOLLAND

Nonnegative Elements of Subgroups of $\mathbb{Z}^n$

J. C. Rosales and Pedro A. García-Sánchez*
Universidad de Granada
Departamento de Álgebra
E-18071 Granada, España

Submitted by Jose A. Dias da Silva

ABSTRACT

We give a method to compute all nonnegative integer solutions of a homogeneous system of linear equations. We use this method to provide an algorithm to compute all nonnegative integer solutions of homogeneous systems of equations having some of the equations in congruences. © 1998 Elsevier Science Inc.

INTRODUCTION

Given a system $Ax = b$ of m linear equations in n indeterminates with integer coefficients, it can be shown, using Cramer's rule, that if the system is solvable then it has a solution whose coordinates are integer numbers bounded by the maximum of the absolute values of the $r \times r$ minors (with $r = \operatorname{rank}(A)$) of the augmented matrix $(A\ b)$ (since we are going to refer to this quantity later, we denote it by D). The question of the size of the "smallest" integer solution of a system of linear equations with integer coefficients is important in the theory of diophantine approximations and in complexity theory. Siegel showed in [7] that if the system is homogeneous ($b = 0$) and $n > m$, then the system admits an integer solution with coordinates bounded by $1 + (nB)^{m/(n-m)}$, where B is a bound for the coefficients of the system of equations. For the nonhomogeneous case ($b \neq 0$), Borosh

*E-mail: jrosales@ugr.es, pedro@goliat.ugr.es.

LINEAR ALGEBRA AND ITS APPLICATIONS 270:351–357 (1998)

0024-3795/98/$19.00
PII S0024-3795(97)00309-1

et al. show in [2] that a bound for the coordinates of an integer solution is D. Besides, one can find the set of all integer solutions of the homogeneous system $Ax = 0$ using, for example, the algorithm to compute the normal Hermite form of A or the LLL algorithm presented in [4].

In this paper, we study the problem of finding all the solutions of $Ax = 0$ with nonnegative integer coordinates. In order to achieve a method to solve this problem, we compute a minimal generating system for this set of solutions, that is to say, a set of solutions $\{s_1, \ldots, s_t\}$ satisfying the condition that every nonnegative interger solution of $Ax = 0$ belongs to $\langle s_1, \ldots, s_t \rangle = \{\sum_{i=1}^{t} a_i s_i \mid a_i \in \mathbb{N}\}$ (where $\mathbb{N}$ stands for the set of nonnegative integers), and such that no other proper subset of $\{s_1, \ldots, s_t\}$ fulfills the same condition. We show that the elements $s_1, \ldots, s_t$ can be found in the set of integer vectors $(x_1, \ldots, x_n)$ such that $x_1 + \cdots + x_n \leqslant (r-1)(n-r)D$. The problem of determining how "small" nonnegative integer solutions of $Ax = 0$ can be has been studied by Borosh in [1], where it is shown that if the system is solvable, then it admits a solution whose coordinates are nonnegative integers less than D.

We extend the method just described to solve the problem of finding nonnegative integer solutions of homogeneous systems of linear equations with integer coefficients, where some or all of the equations are in the form of congruences. This is equivalent to finding a system of generators for the semigroups of the form $M \cap \mathbb{N}^n$, with M an additive subgroup of $\mathbb{Z}^n$ (where, as usual, $\mathbb{Z}$ denotes the set of integers). This class of semigroups coincides, up to isomorphism, with the class of normal semigroups. The importance of normal semigroups is due to the fact that if S is a normal semigroup and K is a field, then the semigroup ring $K[S] = \oplus_{s \in S} Ky^s$ is Cohen-Macaulay (see [3] and [6]).

1. COMPUTING THE NONNEGATIVE SOLUTIONS OF A HOMOGENEOUS SYSTEM WITH INTEGER COEFFICIENTS

In this section, we study the semigroups of the form $S = M \cap \mathbb{N}^n$ with M a subgroup of $\mathbb{Z}^n$ whose defining equations are homogeneous, i.e., of the form

$$Ax = (c_1 \quad \cdots \quad c_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

with $c_i \in \mathbb{Z}^m$ for some positive integer m. Note that S is the set of nonnegative integer solutions of this system of equations.

We are going to give a method to compute a minimal system of generators for S, which is based on the next result and certain bounds which arise in the study of complexity problems related to binomial ideals.

LEMMA 1. *Let $\{s_1, \ldots, s_t\}$ be the set of minimals of $S \setminus \{0\}$ (with respect to the usual ordering in $\mathbb{N}^n$: $a \leqslant b$ if and only if $b - a \in \mathbb{N}^n$). Then*

$$S = \langle s_1, \ldots, s_t \rangle.$$

Proof. Let $s \in S$. If $s \neq 0$, then there exists $i \in \{1, \ldots, t\}$ such that $s_i \leqslant s$. Hence, by definition of $\leqslant$, we have $s - s_i \in \mathbb{N}^k$ and therefore $s - s_i \in S$, because $s - s_i$ belongs also to M. Now, if $s - s_i$ is not zero we can proceed as before. This process must stop, because otherwise we would have an infinite descending chain with respect to $\leqslant$, which is not possible. When this process stops, it is because the resulting element is zero, and this gives us the expression $s - \sum a_i s_i = 0$ and therefore $s \in \langle s_1, \ldots, s_t \rangle$. ■

Thus, if we want to know all nonnegative integer solutions of the system $Ax = 0$, it is enough to find the minimal nontrivial solutions which are in $\mathbb{N}^n$. We are going to show that these minimal elements are in a finite set which can be easily constructed. In order to do that, we need some results concerning binomial ideals and presentations of semigroups.

The map

$$\varphi : \mathbb{N}^n \to S' = \langle c_1, \ldots, c_n \rangle \subseteq \mathbb{Z}^m,$$

$$\varphi(a_1, \ldots, a_n) = \sum a_i c_i$$

induces the following morphism of K-algebras:

$$\bar{\varphi} : K[x_1, \ldots, x_n] \to K[S'],$$

$$\bar{\varphi}(X^a) = y^{\varphi(a)}$$

with kernel (see [5])

$$I_{S'} = \langle X^a - X^b : (a, b) \in \sim_M \rangle,$$

where $\sim_M = \{(a, b) \in \mathbb{N}^{2n} : a - b \in M\}$.

Note that $S = [0]$, where $[0]$ denotes the zero class in $\mathbb{N}^n / \sim_M$. That is to say, if we take and element $s \in S$, then $(s, 0) \in \sim_M$, and if we take an element $(s, 0) \in \sim_M$, then s must be in S.

Given an element $u \in M$, it can be written as $u = u^+ - u^-$, with u^+, $u^- \in \mathbb{N}^n$. Thus, for any $u \in M$, we have that $X^{u^+} - X^{u^-} \in I_{S'}$. Besides, if $X^a - X^b \in I_{S'}$, then $a - b \in M$.

DEFINITION 2. An element $X^{u^+} - X^{u^-} \in I_{S'}$ is called primitive if there exists no other element $X^{v^+} - X^{v^-} \in I_{S'}$ such that X^{v^+} divides X^{u^+} and X^{v^-} divides X^{u^-}.

Note that if s is a minimal element in S, then $X^s - 1 \in I_{S'}$ is primitive. This fact is going to give us the key to compute the minimal elements in S, as the next theorem shows:

THEOREM 3 (Theorem 4.7 in [8]). *Let* rank $A = r$ *and* $D = \max\{|\det(c_{i_1}, \ldots, c_{i_r})| : 1 \leqslant i_1 < \cdots < i_r \leqslant r\}$. *The total degree of any primitive binomial in* $I_{S'}$ *is less than* $(r + 1)(n - r)D$.

Now, since if $s \in S$ is a minimal element then $X^s - 1 \in I_{S'}$ is a primitive element, we have that if $s = (a_1, \ldots, a_n)$ then $\sum_{i=1}^n a_i \leqslant C = (r + 1)(n - r)D$. Note that r and D are easy to compute. This enables us to calculate the minimals of S, since we only have to sweep a finite region, the one bounded by the condition of having total degree C. Note also, that we can always assume that $m = r$.

EXAMPLE 4. Let M be the abelian group whose equations are

$$x + y - z - t = 0,$$

$$2x - 5z = 0.$$

The semigroup S' is generated by $\{(1, 2), (1, 0), (-1, -5), (-1, 0)\}$. The maximum absolute value of the determinants is $D = 5$, and therefore, $C = 3 \times 2 \times 5 = 30$. Hence, the region to sweep is $\{(x, y, z, t) \in \mathbb{N}^4: x + y + z + t \leqslant 30\}$, and the elements in this region are

$\{(0, 0, 0, 0), (0, 1, 0, 1), (0, 2, 0, 2), (0, 3, 0, 3), (0, 4, 0, 4), (0, 5, 0, 5),$
$(0, 6, 0, 6), (0, 7, 0, 7), (0, 8, 0, 8), (0, 9, 0, 9), (0, 10, 0, 10), (0, 11, 0, 11).$
$(0, 12, 0, 12), (0, 13, 0, 13), (0, 14, 0, 14), (0, 15, 0, 15), (5, 0, 2, 3),$
$(5, 1, 2, 4), (5, 2, 2, 5), (5, 3, 2, 6), (5, 4, 2, 7), (5, 5, 2, 8), (5, 6, 2, 9),$
$(5, 7, 2, 10), (5, 8, 2, 11), (5, 9, 2, 12), (5, 10, 2, 13), (10, 0, 4, 6), (10, 1, 4, 7),$
$(10, 2, 4, 8), (10, 3, 4, 9), (10, 4, 4, 10), (10, 5, 4, 11), (15, 0, 6, 9)\}.$

The minimals of this set (excluding the zero element) are $\{(0, 1, 0, 1), (5, 0, 2, 3)\}$. Thus $S = \langle (0, 1, 0, 1), (5, 0, 2, 3) \rangle$.

2. COMPUTING THE NONNEGATIVE ELEMENTS OF A SUBGROUP OF $\mathbb{Z}^n$

Now, the problem is to compute the solutions with nonnegative coordinates of a system of equations of the form

$$\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n &\equiv 0 \pmod{d_1},\\
&\vdots\\
a_{r1}x_1 + \cdots + a_{rn}x_n &\equiv 0 \pmod{d_r},\\
a_{r+1\,1}x_1 + \cdots + a_{4+1\,n}x_n &= 0,\\
&\vdots\\
a_{r+k\,1}x_1 + \cdots + a_{r+k\,n}x_n &= 0.
\end{aligned}$$

If we denote by $M \subseteq \mathbb{Z}^n$ the set of solutions of this system, the problem we want to solve is to compute a system of generators of the affine semigroup $M \cap \mathbb{N}^n$. It is easy to show that this kind of semigroup is also generated by its minimals, as we did in Lemma 1.

We are going to transform the above system of equations into a system of linear equations without congruences, and then apply the results given in the

last section. Then, we will show how to reconstruct the nonnegative integer solutions of the former system of equations from the solutions of the new system of equations. Let M' be the set of the solutions of the system of equations

$$\begin{aligned}
a_{11}x_1 + \cdots + a_{1n}x_n + d_1y_1 - d_1z_1 &= 0,\\
&\vdots\\
a_{r1}x_1 + \cdots + a_{rn}x_n + d_ry_r - d_rz_r &= 0,\\
a_{r+11}x_1 + \cdots + a_{r+1n}x_n &= 0,\\
&\vdots\\
a_{r+k1}x_1 + \cdots + a_{r+kn}x_n &= 0.
\end{aligned}$$

We can compute a system of generators of the semigroup $S' = \mathbb{N}^{n+2r} \cap M'$ using what we already know for linear systems of homogeneous equations.

Let us denote by π the projection

$$\pi : \mathbb{N}^{n+2r} \to \mathbb{N}^n,$$

$$\pi(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+2r}) = (a_1, \ldots, a_n).$$

If $s = (a_1, \ldots, a_n) \in S$, then

$$a_{il}x_1 + \cdots + a_{in}x_n = k_id_i$$

for all $i \in \{1, \ldots, r\}$. We define

$$b_i = \begin{cases} 0 & \text{if } k_i \geqslant 0,\\ -k_i & \text{otherwise,} \end{cases} \qquad c_i = \begin{cases} k_i & \text{if } k_i \geqslant 0,\\ 0 & \text{otherwise.} \end{cases}$$

Take $s' = (a_1, \ldots, a_n, b_1, \ldots, b_r, c_1, \ldots, c_r)$. Clearly, $s' \in S'$ and $\pi(s') = s$. If $S' = \langle s'_1, \ldots, s'_m \rangle$, then there exist $l_1, \ldots, l_m \in \mathbb{N}$ such that $s' = \sum l_i s'_i$. Thus, $s = \pi(s') = \sum l_i \pi(s'_i)$. This shows that S can be generated by $\{\pi(s'_1), \ldots, \pi(s'_m)\}$.

REFERENCES

1 I. Borosh, A sharp bound for positive solutions of homogeneous linear diophantine equations, *Proc. Amer. Math. Soc.* 60:19–21 (1976).
2 I. Borosh, M. Flahive, D. Rubin, and B. Treybig, A sharp bound for solutions of linear diophantine equations, *Proc. Amer. Math. Soc.* 105:844–846 (1989).
3 W. Burns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Stud. Adv. Math. 39, Cambridge U.P.
4 H. Cohen, *A Course on Computational Algebraic Number Theory*, Springer-Verlag, 1993.
5 J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math* 3:175–193 (1970).
6 M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes, *Ann. of Math.* 96:318–337 (1972).
7 C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuß. Akad. Wiss. Phys.-Math. Kl*, 1929, No. 1; in *Ges. Abh.*, Vol. I, pp. 209–266.
8 B. Sturmfels, *Gröbner Bases and Convex Polytopes*, Expanded lecture notes from the Holiday Symposium at New Mexico State University, Las Cruces, 27–31 Dec., 1994.

Received 4 December 1996; final manuscript accepted 26 June 1997